Payment Card Industry

Data Security Standard

Attestation of Compliance for Report on Compliance – Service Providers

Version 4.0.1

Publication Date: August 2024

PCI DSS v4.0.1 Attestation of Compliance for Report on Compliance – Service Providers

Entity Name: Auction Ninja

Date of Report as noted in the Report on Compliance: December 20th 2025

Date Assessment Ended: 10th December 2025

Section 1: Assessment Information

Instructions for Submission

This Attestation of Compliance (AOC) must be completed as a declaration of the results of the service provider's assessment against the *Payment Card Industry Data Security Standard (PCI DSS) Requirements and Testing Procedures (*"Assessment"). Complete all sections. The service provider is responsible for ensuring that each section is completed by the relevant parties, as applicable. Contact the entity(ies) to which this AOC will be submitted for reporting and submission procedures.

This AOC reflects the results documented in an associated Report on Compliance (ROC). Associated ROC sections are noted in each AOC Part/Section below.

Capitalized terms used but not otherwise defined in this document have the meanings set forth in the PCI DSS Report on Compliance Template.

Part 1. Contact Information

	Part 1a. Assessed Entity (ROC Section 1.1)	
	Company name:	Auction Ninja LLC
	DBA (doing business as):	
	Company mailing address:	1720 Fairfield Avenue | Bridgeport, CT 06605
	Company main website:	https://www.auctionninja.com/
	Company contact name:	Rae Parth
	Company contact title:	CTO
	Contact phone number:	
	Contact e-mail address:	rp@auctionninja.com

Part 1b. Assessor (ROC Section 1.1)

Provide the following information for all assessors involved in the Assessment. If there was no assessor for a given assessor type, enter Not Applicable.

	PCI SSC Internal Security Assessor(s)	
	ISA name(s):	Not Applicable
	Qualified Security Assessor	
	Company name:	Not Applicable
	Company mailing address:	Not Applicable
	Company website:	Not Applicable
	Lead Assessor name:	Not Applicable
	Assessor phone number:	Not Applicable
	Assessor e-mail address:	Not Applicable

Assessor certificate number:	

Part 2. Executive Summary

Part 2a. Scope Verification

Services that were INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) assessed:	AuctionNinja Website

Type of service(s) assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☒ Applications / software	☐ Systems security services	☐ POI / card present
☐ Hardware	☐ IT support	☐ Internet / e-commerce
☐ Infrastructure / Network	☐ Physical security	☐ MOTO / Call Center
☐ Physical space (co-location)	☐ Terminal Management System	☐ ATM
☐ Storage	☐ Other services (specify):	☐ Other processing (specify):
☐ Web-hosting services		
☐ Security services		
☐ 3-D Secure Hosting Provider		
☐ Multi-Tenant Service Provider		
☐ Other Hosting (specify):		
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

Note: *These categories are provided for assistance only and are not intended to limit or predetermine an entity's service description. If these categories do not apply to the assessed service, complete "Others." If it is not clear whether a category could apply to the assessed service, consult with the entity(ies) to which this AOC will be submitted.*

Part 2. Executive Summary *(continued)*

Part 2a. Scope Verification *(continued)*

Services that are provided by the service provider but were NOT INCLUDED in the scope of the Assessment (select all that apply):

Name of service(s) not assessed:	Not Applicable

Type of service(s) not assessed:

Hosting Provider:	**Managed Services:**	**Payment Processing:**
☐ Applications / software ☐ Hardware ☐ Infrastructure / Network ☐ Physical space (co-location) ☐ Storage ☐ Web-hosting services ☐ Security services ☐ 3-D Secure Hosting Provider ☐ Multi-Tenant Service Provider ☐ Other Hosting (specify):	☐ Systems security services ☐ IT support ☐ Physical security ☐ Terminal Management System ☐ Other services (specify):	☐ POI / card present ☐ Internet / e-commerce ☐ MOTO / Call Center ☐ ATM ☐ Other processing (specify):
☐ Account Management	☐ Fraud and Chargeback	☐ Payment Gateway/Switch
☐ Back-Office Services	☐ Issuer Processing	☐ Prepaid Services
☐ Billing Management	☐ Loyalty Programs	☐ Records Management
☐ Clearing and Settlement	☐ Merchant Services	☐ Tax/Government Payments
☐ Network Provider		
☐ Others (specify):		

Provide a brief explanation why any checked services were not included in the Assessment:	Not Applicable

Part 2b. Description of Role with Payment Cards (ROC Sections 2.1 and 3.1)

Describe how the business stores, processes, and/or transmits account data.	AuctionNinja does **not store, process, or retain** full Primary Account Number (PAN) data. Payment card data is **collected from customers via the AuctionNinja web application and transmitted directly to a PCI DSS–compliant third-party payment service provider (Stripe) using secure, encrypted API connections**. All transmission of account data is protected using industry-standard encryption (TLS). AuctionNinja does not store sensitive authentication data (such as CVV) at any time. Any payment-related tokens returned by the payment service provider are non-sensitive and cannot be used to reconstruct PAN.
Describe how the business is otherwise involved in or has the ability to impact the security of its customers' account data.	AuctionNinja's involvement with account data is limited to **securely collecting payment information from customers through its web application and**

	transmitting it to the third-party payment service provider. While AuctionNinja does not store account data, it can **impact the security of PAN data during collection and transmission**, including: • The security of the web application used to capture payment data • The integrity of client-side and server-side code handling payment requests • The security configuration of systems and networks that transmit data to the payment service provider AuctionNinja maintains security controls to reduce the risk of interception or manipulation of account data during transit.
Describe system components that could impact the security of account data.	The following system components could impact the security of account data: • AuctionNinja web application (client-side and server-side components involved in payment collection) • Backend application servers that handle payment requests and API calls • Network infrastructure used to transmit data to the payment service provider • Security controls protecting these systems (e.g., access controls, encryption, monitoring) These components are managed and secured to support the confidentiality and integrity of account data during transmission.

Part 2. Executive Summary *(continued)*

Part 2c. Description of Payment Card Environment

Provide a high-level description of the environment covered by this Assessment. *For example:* • *Connections into and out of the cardholder data environment (CDE).*	The environment covered by this PCI DSS assessment includes the application and supporting infrastructure used to collect and

- *Critical system components within the CDE, such as POI devices, databases, web servers, etc., and any other necessary payment components, as applicable.*
- *System components that could impact the security of account data.*

transmit payment card data through the **AuctionNinja** platform.

Hosting and Architecture

The AuctionNinja application environment is hosted by the cloud service provider **HostDime**. The environment consists of publicly accessible web servers, backend application servers, and supporting network infrastructure required to operate the AuctionNinja platform.

Cardholder Data Flow and CDE Scope

Cardholder Data (CHD) is collected exclusively through the AuctionNinja web application in accordance with PCI DSS requirements. The platform **does not store full Primary Account Number (PAN), CVV/CVC, or sensitive authentication data**.

AuctionNinja stores only the following limited card-related data elements, where applicable:

- Last four digits of the PAN
- Cardholder name
- Billing address
- Card expiration date

All payment card transactions and full CHD are **securely transmitted directly to a PCI DSS–compliant third-party Payment Service Provider (PSP)** using strong encryption (e.g., TLS). Payment processing, authorization, and storage of full CHD are handled solely by the PSP and are outside the AuctionNinja environment.

Connections Into and Out of the Environment

Key connections include:

- Customer browsers connecting to the AuctionNinja web application over HTTPS

- Secure, encrypted API connections from the AuctionNinja application servers to the third-party PSP
- Administrative access to systems restricted to authorized personnel via secure management interfaces
- Outbound log and monitoring data transmitted to centralized monitoring services

No inbound connections from the PSP into the AuctionNinja environment are permitted.

System Components That Could Impact the Security of Account Data

System components that could impact the security of account data include:

- AuctionNinja web application (client-side and server-side payment collection components)
- Backend application servers handling payment-related requests and API calls
- Network infrastructure (firewalls, routing, and security controls)
- Supporting operating systems and application frameworks

Logging, Monitoring, and Security Controls

Security event logs and application logs related to payment activity and system access are centrally collected and forwarded to **New Relic** for monitoring, alerting, and audit trail purposes, supporting PCI DSS logging and monitoring requirements.

Network and system security controls—including firewalls and intrusion detection and prevention—are implemented and maintained using **Imunify360**. These controls are configured to detect, prevent, and

	respond to malicious activity in alignment with PCI DSS Requirements 1 and 11. **Data Protection and Access Control** All data stored within the AuctionNinja environment, including the limited CHD elements retained, is encrypted at rest using industry-accepted cryptographic standards. Access to systems and data is restricted based on the principle of least privilege, with access rights and security controls reviewed on a regular basis.
Indicate whether the environment includes segmentation to reduce the scope of the Assessment. (Refer to the "Segmentation" section of PCI DSS for guidance on segmentation)	☐ Yes ☒ No

Part 2d. In-Scope Locations/Facilities
(ROC Section 4.6)

List all types of physical locations/facilities (for example, corporate offices, data centers, call centers and mail rooms) in scope for this Assessment.

Facility Type	Total Number of Locations (How many locations of this type are in scope)	Location(s) of Facility (city, country)
Not Applicable	*Not Applicable*	*Not Applicable*

Part 2. Executive Summary *(continued)*

Part 2e. PCI SSC Validated Products and Solutions
(ROC Section 3.3)

Does the entity use any item identified on any PCI SSC Lists of Validated Products and Solutions[1]?

☐ Yes ☒ No

Provide the following information regarding each item the entity uses from PCI SSC's Lists of Validated Products and Solutions:

1

Name of PCI SSC validated Product or Solution	Version of Product or Solution	PCI SSC Standard to which Product or Solution Was Validated	PCI SSC Listing Reference Number	Expiry Date of Listing
Not Applicable	*Not Applicable*	*Not Applicable*	*Not Applicable*	*Not Applicable*

* For purposes of this document, "Lists of Validated Products and Solutions" means the lists of validated products, solutions, and/or components, appearing on the PCI SSC website (www.pcisecuritystandards.org) (for example, 3DS Software Development Kits, Approved PTS Devices, Validated Payment Software, Point to Point Encryption (P2PE) solutions, Software-Based PIN Entry on COTS (SPoC) solutions, Contactless Payments on COTS (CPoC) solutions), and Mobile Payments on COTS (MPoC) products.

Part 2. Executive Summary *(continued)*

Part 2f. Third-Party Service Providers (ROC Section 4.4)

For the services being validated, does the entity have relationships with one or more third-party service providers that:

• Store, process, or transmit account data on the entity's behalf (for example, payment gateways, payment processors, payment service providers (PSPs, and off-site storage))	☒ Yes ☐ No
• Manage system components included in the entity's Assessment (for example, via network security control services, anti-malware services, security incident and event management (SIEM), contact and call centers, web-hosting companies, and IaaS, PaaS, SaaS, and FaaS cloud providers)	☒ Yes ☐ No
• Could impact the security of the entity's CDE (for example, vendors providing support via remote access, and/or bespoke software developers).	☒ Yes ☐ No

If Yes:

Name of Service Provider:	Description of Services Provided:
New Relic	Provides centralized application performance monitoring, infrastructure monitoring, and security-related logging. New Relic is used to collect, retain, and analyze system and application logs related to user activity, administrative access, and payment-related workflows. These logs support security monitoring, alerting, incident investigation, and audit trail requirements in alignment with PCI DSS logging and monitoring controls. New Relic does not process, transmit, or store payment card data.
Security metrics	Provides Approved Scanning Vendor (ASV) services, including quarterly external vulnerability scanning of in-scope internet-facing systems, as required by PCI DSS. Scan results are reviewed and remediated as necessary to maintain compliance with PCI DSS vulnerability management requirements. The ASV does not have access to payment card data.
Host dime	Provides cloud hosting and infrastructure services, including compute resources, storage, networking, and physical data center security for the AuctionNinja application environment. HostDime is responsible for the underlying physical infrastructure and availability of hosted systems. AuctionNinja is responsible for the security configuration of operating systems, applications, and data hosted within the environment in accordance with the shared responsibility model.
Immunify 360	Provides host-based security controls, including firewall capabilities, intrusion detection and prevention (IDS/IPS), malware detection, and automated threat response. Imunify360 is used to protect application servers from malicious activity and to support continuous monitoring and prevention of common attack vectors in alignment with PCI DSS Requirements 1 and 11. Imunify360 does not process or store payment card data.
Stripe, NMI and Authorize.Net	Provides PCI DSS–compliant payment processing services, including secure collection, transmission, authorization, and settlement of payment card transactions. Payment providers handles the processing and storage of full cardholder data, including PAN

	and sensitive authentication data, within its PCI DSS–certified environment. AuctionNinja transmits payment data to Stripe using secure, encrypted connections and does not store or process full cardholder data.

Note: *Requirement 12.8 applies to all entities in this list.*

Part 2. Executive Summary *(continued)*

Part 2g. Summary of Assessment (ROC Section 1.8.1)

Indicate below all responses provided within each principal PCI DSS requirement.

For all requirements identified as either "Not Applicable" or "Not Tested," complete the "Justification for Approach" table below.

Note: *One table to be completed for each service covered by this AOC. Additional copies of this section are available on the PCI SSC website.*

Name of Service Assessed: AuctionNinja website

PCI DSS Requirement	Requirement Finding More than one response may be selected for a given requirement. Indicate all responses that apply.				Select If a Compensating Control(s) Was Used
	In Place	Not Applicable	Not Tested	Not in Place	
Requirement 1:	☒	☐	☐	☐	☐
Requirement 2:	☒	☐	☐	☐	☐
Requirement 3:	☒	☐	☐	☐	☐
Requirement 4:	☒	☐	☐	☐	☐
Requirement 5:	☒	☐	☐	☐	☐
Requirement 6:	☒	☐	☐	☐	☐
Requirement 7:	☒	☐	☐	☐	☐
Requirement 8:	☒	☐	☐	☐	☐
Requirement 9:	☐	☐	☒	☐	☐
Requirement 10:	☒	☐	☐	☐	☐
Requirement 11:	☒	☐	☐	☐	☐
Requirement 12:	☒	☐	☐	☐	☐
Appendix A1:	☒	☐	☐	☐	☐
Appendix A2:	☐	☒	☐	☐	☐

Justification for Approach

For any Not Applicable responses, identify which sub-requirements were not applicable and the reason.	AuctionNinja does **not support card-present transactions** and does **not use Point-of-Interaction (POI) terminals**, payment terminals, or any other card-present devices. All payment card transactions are **card-not-present** and are performed through the AuctionNinja web application. The AuctionNinja environment does **not use SSL or early TLS** protocols for payment processing. All payment data transmissions occur over modern, secure encryption protocols (e.g., TLS 1.2 or higher) between customer browsers, the AuctionNinja platform, and the PCI DSS–compliant third-party payment service provider. Because Appendix A2 applies exclusively to **card-present POS environments using SSL or early TLS for POI terminal connections**, these requirements do not apply to the AuctionNinja environment and were not assessed as part of this review.
For any Not Tested responses, identify which sub-requirements were not tested and the reason.	The AuctionNinja cardholder data environment is hosted entirely within the cloud infrastructure of the third-party cloud service provider **HostDime**. AuctionNinja does not own, operate, or maintain any physical facilities, data centers, servers, or storage devices that store or process cardholder data. Physical access controls—including facility access restrictions, visitor management, media handling, and physical security monitoring—are the responsibility of HostDime under the shared responsibility model. As a result, physical security controls applicable to PCI DSS Requirement 9 fall outside the scope of AuctionNinja's assessment and were not tested as part of this review. HostDime is responsible for maintaining appropriate physical security controls for its data centers in accordance with applicable compliance and contractual requirements.

Section 2 Report on Compliance

(**ROC Sections 1.2 and 1.3**)

Date Assessment began: ***Note:*** *This is the first date that evidence was gathered, or observations were made.*	2025-08-5
Date Assessment ended: ***Note:*** *This is the last date that evidence was gathered, or observations were made.*	2025-12-10
Were any requirements in the ROC unable to be met due to a legal constraint?	☐ Yes ☒ No
Were any testing activities performed remotely?	☒ Yes ☐ No

Section 3 Validation and Attestation Details

Part 3. PCI DSS Validation (ROC Section 1.7)

This AOC is based on results noted in the ROC dated *(Date of Report as noted in the ROC YYYY-MM-DD)*.

Indicate below whether a full or partial PCI DSS assessment was completed:

☐ **Full Assessment** – All requirements have been assessed and therefore no requirements were marked as Not Tested in the ROC.

☒ **Partial Assessment** – One or more requirements have not been assessed and were therefore marked as Not Tested in the ROC. Any requirement not assessed is noted as Not Tested in Part 2g above.

Based on the results documented in the ROC noted above, each signatory identified in any of Parts 3b-3d, as applicable, assert(s) the following compliance status for the entity identified in Part 2 of this document *(select one)*:

☒	**Compliant:** All sections of the PCI DSS ROC are complete, and all assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above.
☐	**Non-Compliant:** Not all sections of the PCI DSS ROC are complete, or one or more requirements are marked as Not in Place, resulting in an overall **NON-COMPLIANT** rating; thereby *(Service Provider Company Name)* has not demonstrated compliance with PCI DSS requirements. **Target Date** for Compliance: *YYYY-MM-DD* An entity submitting this form with a Non-Compliant status may be required to complete the Action Plan in Part 4 of this document. Confirm with the entity to which this AOC will be submitted before completing Part 4.
☐	**Compliant but with Legal exception:** One or more assessed requirements in the ROC are marked as Not in Place due to a legal restriction that prevents the requirement from being met and all other assessed requirements are marked as being either In Place or Not Applicable, resulting in an overall **COMPLIANT BUT WITH LEGAL EXCEPTION** rating; thereby *(Service Provider Company Name)* has demonstrated compliance with all PCI DSS requirements except those noted as Not Tested above or as Not in Place due to a legal restriction. This option requires additional review from the entity to which this AOC will be submitted. *If selected, complete the following:*

Affected Requirement	Details of how legal constraint prevents requirement from being met

Part 3. PCI DSS Validation *(continued)*

Part 3a. Service Provider Acknowledgement

Signatory(s) confirms:

(Select all that apply)

☒	The ROC was completed according to *PCI DSS*, Version 4.0.1 and was completed according to the instructions therein.
☒	All information within the above-referenced ROC and in this attestation fairly represents the results of the Assessment in all material respects.
☒	PCI DSS controls will be maintained at all times, as applicable to the entity's environment.

Part 3b. Service Provider Attestation

Rae Parth

Signature of Service Provider Executive Officer	Date: 01-15-2026
Service Provider Executive Officer Name:	Title:CTO

Rae Parth

Part 3c. Qualified Security Assessor (QSA) Acknowledgement

If a QSA was involved or assisted with this Assessment, indicate the role performed:	☐ QSA performed testing procedures.
	☐ QSA provided other assistance. If selected, describe all role(s) performed:

Signature of Lead QSA	Date: YYYY-MM-DD
Lead QSA Name:	

Signature of Duly Authorized Officer of QSA Company	Date: YYYY-MM-DD
Duly Authorized Officer Name:	QSA Company:

Part 3d. PCI SSC Internal Security Assessor (ISA) Involvement

If an ISA(s) was involved or assisted with this Assessment, indicate the role performed:	☐ ISA(s) performed testing procedures.
	☐ ISA(s) provided other assistance. If selected, describe all role(s) performed:

Part 4. Action Plan for Non-Compliant Requirements

Only complete Part 4 upon request of the entity to which this AOC will be submitted, and only if the Assessment has Non-Compliant results noted in Section 3.

If asked to complete this section, select the appropriate response for "Compliant to PCI DSS Requirements" for each requirement below. For any "No" responses, include the date the entity expects to be compliant with the requirement and provide a brief description of the actions being taken to meet the requirement.

PCI DSS Requirement	Description of Requirement	Compliant to PCI DSS Requirements (Select One)		Remediation Date and Actions (If "NO" selected for any Requirement)
		YES	NO	
1	Install and maintain network security controls	☐	☐	Not Applicable
2	Apply secure configurations to all system components	☐	☐	Not Applicable
3	Protect stored account data	☐	☐	Not Applicable
4	Protect cardholder data with strong cryptography during transmission over open, public networks	☐	☐	Not Applicable
5	Protect all systems and networks from malicious software	☐	☐	Not Applicable
6	Develop and maintain secure systems and software	☐	☐	Not Applicable
7	Restrict access to system components and cardholder data by business need to know	☐	☐	Not Applicable
8	Identify users and authenticate access to system components	☐	☐	Not Applicable
9	Restrict physical access to cardholder data	☐	☐	Not Applicable
10	Log and monitor all access to system components and cardholder data	☐	☐	Not Applicable
11	Test security systems and networks regularly	☐	☐	Not Applicable
12	Support information security with organizational policies and programs	☐	☐	Not Applicable
Appendix A1	Additional PCI DSS Requirements for Multi-Tenant Service Providers	☐	☐	Not Applicable
Appendix A2	Additional PCI DSS Requirements for Entities using SSL/early TLS for Card-Present POS POI Terminal Connections	☐	☐	Not Applicable

Note: The PCI Security Standards Council is a global standards body that provides resources for payment security professionals developed collaboratively with our stakeholder community. Our materials are accepted in numerous compliance programs worldwide. Please check with your individual compliance accepting organization to ensure that this form is acceptable in their program. For more information about PCI SSC and our stakeholder community please visit:

https://www.pcisecuritystandards.org/about_us/